PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-078159
(43)Date of publication of application : 23.03.2001

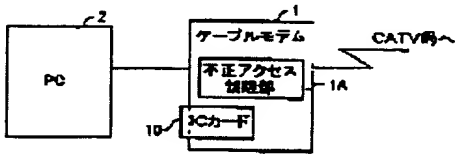
(51)Int.Cl. H04N 7/10
H04L 12/56
H04N 7/16

(21)Application number : 11-253668
(22)Date of filing : 07.09.1999

(71)Applicant : NEC CORP
(72)Inventor : OGAWA EMI

(54) UNAUTHORIZED ACCESS LIMIT SYSTEM TO CABLE MODEM AND METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To limit a malicious unauthorized access to a cable MODEM, where an access request source is not identified.
SOLUTION: The cable MODEM unauthorized access limit system where a personal computer under the management of a head end MODEM of a CATV station is accessed, is provided with an IC card 10 to which access permission IP addresses whose access is permitted are registered and that is mounted on a cable MODEM and with an unauthorized access limit section 1A that rejects an access by discriminating it to be an unauthorized access when an IP address of an access request source is dissident with any of the access permission IP addresses registered in the IC card 10.



LEGAL STATUS

[Date of request for examination]	08.08.2000
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	3546771
[Date of registration]	23.04.2004
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－78159
（P2001－78159A）
(43)公開日　平成13年３月23日(2001.3.23)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'（参考）
Ｈ０４Ｎ　7/10		Ｈ０４Ｎ　7/10		５Ｃ０６４
Ｈ０４Ｌ　12/56			7/16	Ａ　５Ｋ０３０
Ｈ０４Ｎ　7/16		Ｈ０４Ｌ　11/20		１０２Ａ　９Ａ００１

審査請求　有　　請求項の数６　ＯＬ　（全　６　頁）

(21)出願番号　特願平11－253668

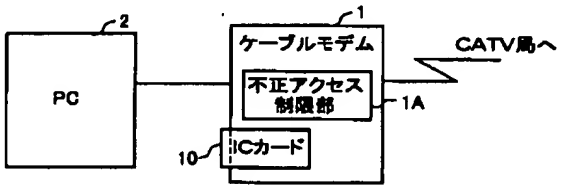
(22)出願日　平成11年９月７日(1999.9.7)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(72)発明者　小川　恵美
東京都港区芝五丁目７番１号　日本電気株式会社内
(74)代理人　100104400
弁理士　浅野　雄一郎

Ｆターム(参考)　5C064 BA01 BB05 BB07 BB10 BC06
BC10 BC20 BC27 BD01 BD07
5K030 GA15 HC01 JA09 LC18 LD07
9A001 CC02 JJ25 JJ27 LL03

(54)【発明の名称】　ケーブルモデムの不正アクセス制限システム及び方法

(57)【要約】
【課題】　アクセス要求元が不明で悪意のある不正アクセスを制限する。
【解決手段】　ＣＡＴＶ局のヘッドエンドモデム配下のパーソナルコンピュータにアクセスするケーブルモデムの不正アクセス制限システムに、アクセスを許可するアクセス許可ＩＰアドレスが登録され、前記ケーブルモデムに実装されるＩＣカード１０と、アクセス要求元のＩＰアドレスが前記ＩＣカードに登録されているアクセス許可ＩＰアドレスと一致しない場合には不正アクセスとしてアクセスを拒否する不正アクセス制限部１Ａとを備える。



1

【特許請求の範囲】

【請求項１】　ＣＡＴＶ局のヘッドエンドモデム配下のパーソナルコンピュータにアクセスするケーブルモデムの不正アクセス制限システムにおいて、アクセスを許可するアクセス許可ＩＰアドレスが登録され前記ケーブルモデムに実装されるＩＣカードと、

アクセス要求元のＩＰアドレスが前記ＩＣカードに登録されているアクセス許可ＩＰアドレスと一致しない場合には不正アクセスとしてアクセスを拒否する不正アクセス制限部とを備えることを特徴とするケーブルモデムの不正アクセス制限システム。

【請求項２】　前記不正アクセス制限部はアクセス要求元のＩＰアドレスが前記ＩＣカードに登録されているアクセス許可ＩＰアドレスと一致しない場合には受信したデータを廃棄することを特徴とする、請求項１に記載のケーブルモデムの不正アクセス制限システム。

【請求項３】　前記不正アクセス制限部は前記ケーブルモデムに前記ＩＣカードが挿入されている場合のみアクセス拒否の判断を行うことを特徴とする、請求項１に記載のケーブルモデムの不正アクセス制限システム。

【請求項４】　前記ＩＣカードは不正アクセス履歴テーブルを保持し、前記不正アクセス履歴テーブルにはアクセス要求元のＩＰアドレス、不正アクセス回数が記憶され、前記不正アクセス制限部は前記不正アクセス履歴テーブルを参照して、不正アクセス回数が所定回数を超える場合には、アクセス要求元のＩＰアドレスを管理者に通知することを特徴とする、請求項１に記載のケーブルモデムの不正アクセス制限システム。

【請求項５】　前記ヘッドエンドモデムにはサーバーが接続され、前記サーバーは前記パーソナルコンピュータからの要求に対して、ユーザＩＤを確認して、前記ＩＣカードのアクセス許可ＩＰアドレスの書き換えを行うことを特徴とする、請求項１に記載のケーブルモデムの不正アクセス制限システム。

【請求項６】　ＣＡＴＶ局のヘッドエンドモデム配下のパーソナルコンピュータにアクセスするケーブルモデムの不正アクセス制限方法において、

アクセスを許可するアクセス許可ＩＰアドレスが登録されるＩＣカードを前記ケーブルモデムに実装する工程と、

アクセス要求元のＩＰアドレスが前記ＩＣカードに登録されているアクセス許可ＩＰアドレスと一致しない場合には不正アクセスとしてアクセスを拒否する工程とを備えることを特徴とするケーブルモデムの不正アクセス制限方法。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は双方向ＣＡＴＶ回線に関する。特に、本発明は、ユーザ宅内のケーブルモデムへの不正アクセス制限システムに関する。

2

【０００２】

【従来の技術】図７は双方向ＣＡＴＶ回線を使ったネットワークを示す図である。本図に示すように、ヘッドエンドモデム２１には複数のケーブルモデル２３、２７が接続され、ケーブルモデム２３、２７にはＰＣ（パーソナルコンピュータ）２５、２９がそれぞれ接続される。

【０００３】他方、ヘッドエンドモデム２２には複数のケーブルモデル２４、２８が接続され、ケーブルモデム２４、２８にはＰＣ２６、３０がそれぞれ接続される。ヘッドエンドモデム２１、２２は相互に接続され、例えば、ＰＣ２５からＰＣ２６へ又はこの逆に、双方向の通信が可能である。

【０００４】さらに、ヘッドエンドモデム２１、２２の各々はインターネットにも接続される。なお、ケーブルモデムは、標準仕様のＤＯＣＳＩＳ（Ｄａｔａ－Ｏｖｅｒ－Ｃａｂｌｅ Ｓｅｒｖｉｃｅ Ｉｎｔｅｒｆａｃｅ Ｓｐｅｃｉｆｉｃａｔｉｏｎｓ）が使用され、常時接続が特徴である。

【０００５】

【発明が解決しようとする課題】ところで、上記双方向ＣＡＴＶ回線では、複数台のヘッドエンドモデムがネットワーク内に存在する場合、異なるヘッドエンドモデム配下のＰＣ間で、自由にアクセスが可能となる。このため、アクセス要求元が不明で悪意のある不正アクセスが可能になるという問題がある。

【０００６】すなわち、ケーブルモデムは標準仕様のＤＯＣＳＩＳだけでは、外部からの不正アクセスに対するセキュリティ機能が十分ではない。また、ネットワーク内に複数台のヘッドエンドアクセスが存在する場合のセキュリティ機能も十分ではない。したがって、本発明は上記問題点に鑑みて、アクセス要求元が不明で悪意のある不正アクセスを制限するケーブルモデムの不正アクセス制限システム及び方法を提供することを目的とする。

【０００７】

【課題を解決するための手段】本発明は前記問題点を解決するために、ＣＡＴＶ局のヘッドエンドモデム配下のパーソナルコンピュータにアクセスするケーブルモデムの不正アクセス制限システムにおいて、アクセスを許可するアクセス許可ＩＰアドレスが登録され前記ケーブルモデムに実装されるＩＣカードと、アクセス要求元のＩＰアドレスが前記ＩＣカードに登録されているアクセス許可ＩＰアドレスと一致しない場合には不正アクセスとしてアクセスを拒否する不正アクセス制限部とを備えることを特徴とするケーブルモデムの不正アクセス制限システムを提供する。

【０００８】この手段により、複数台のヘッドエンドモデムがネットワーク内に存在する場合に、異なるヘッドエンドモデム配下のＰＣ間でアクセスの制限を行うようにしたので、アクセス要求元が不明で悪意のある不正アクセスを制限することが可能になる。好ましくは、前記

不正アクセス制限部はアクセス要求元のＩＰアドレスが前記ＩＣカードに登録されているアクセス許可ＩＰアドレスと一致しない場合には受信したデータを廃棄する。

【０００９】この手段により、受信したデータにより悪影響を受ける可能性を回避するためである。好ましくは、前記不正アクセス制限部は前記ケーブルモデムに前記ＩＣカードが挿入されている場合のみアクセス拒否の判断を行う。この手段により、ＩＣカードの有無によるユーザ毎のサービス（セキュリティー機能の有無）の設定を可能にする。

【００１０】好ましくは、前記ＩＣカードは不正アクセス履歴テーブルを保持し、前記不正アクセス履歴テーブルにはアクセス要求元のＩＰアドレス、不正アクセス回数が記憶され、前記不正アクセス制限部は前記不正アクセス履歴テーブルを参照して、不正アクセス回数が所定回数を超える場合には、アクセス要求元のＩＰアドレスを管理者に通知する。

【００１１】この手段により、繰り返し不正アクセスを制限するためである。好ましくは、前記ヘッドエンドモデムにはサーバーが接続され、前記サーバーは前記パーソナルコンピュータからの要求に対して、ユーザＩＤを確認して、前記ＩＣカードのアクセス許可ＩＰアドレスの書き換えを行う。この手段により、アクセス許可ＩＰアドレスの変更を容易に行うことができるようになった。

【００１２】さらに、本発明は、ＣＡＴＶ局のヘッドエンドモデム配下のパーソナルコンピュータにアクセスするケーブルモデムの不正アクセス制限方法において、アクセスを許可するアクセス許可ＩＰアドレスが登録されるＩＣカードを前記ケーブルモデムに実装する工程と、アクセス要求元のＩＰアドレスが前記ＩＣカードに登録されているアクセス許可ＩＰアドレスと一致しない場合には不正アクセスとしてアクセスを拒否する工程とを備えることを特徴とするケーブルモデムの不正アクセス制限方法を提供する。

【００１３】この手段により、上記発明と同様に、複数台のヘッドエンドモデムがネットワーク内に存在する場合に、異なるヘッドエンドモデム配下のＰＣ間でアクセスの制限を行うようにしたので、アクセス要求元が不明で悪意のある不正アクセスを制限することが可能になる。

【００１４】

【発明の実施の形態】以下、本発明の実施の形態について図面を参照して説明する。図１は本発明に係るケーブルモデムの不正アクセス制限システムの概略構成を示すブロック図である。本図に示すように、ケーブルモデムの不正アクセス制限システムを構成するケーブルモデム１はＤＯＣＳＩＳ仕様であり、外部のＣＡＴＶ（Ｃａｂｌｅ　Ｔｅｌｅｖｉｓｉｏｎ）局に接続される。

【００１５】また、ケーブルモデム１にはＩＣ（Ｉｎｔｅｇｒａｔｅｄ　Ｃｉｒｃｕｉｔ）カード１０が実装され、ＩＣカード１０にはアクセスを許可すべきアクセス許可ＩＰ（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）アドレスが登録されている。また、ＩＣカード１０には不正アクセス履歴テーブルが保持され、不正アクセス履歴テーブルは、アクセスが許可されたＩＰアドレス以外のアクセスを不正アクセスとして、不正アクセスが行われたＩＰアドレスを登録する。

【００１６】さらに、ケーブルモデム１には不正アクセス制限部１Ａが設けられ、不正アクセス制限部１Ａは、アクセス要求元のＩＰアドレスがＩＣカード１０に登録されているアクセス許可ＩＰアドレスと一致しない場合には、アクセスを拒否する。さらに、不正アクセス制限部１Ａは、ＩＣカード１０の不正アクセス履歴を参照して不正アクセス回数が多い場合には、アクセス要求元のＩＰアドレスを後述するサーバー４に通知する。

【００１７】さらに、ケーブルモデム１には、１０Ｂａｓｅ又はＵＳＢ（Ｕｎｉｖｅｒｓａｌ　Ｓｅｒｉａｌ　Ｂｕｓ）を介して、ＰＣ（パーソナルコンピュータ）２が接続されている。ケーブルモデム１の配下のＰＣ２はＩＣカード１０内に登録されているアクセス許可ＩＰアドレスを追加し、修正し、削除することを、後述するサーバー４へ要求する。

【００１８】図２は図１のケーブルモデム１に接続されるＣＡＴＶを説明する図である。本図に示すように、ＩＣカード１０が実装されるケーブルモデム１、ＰＣ２はユーザ宅内に設置され、ケーブルモデム１にはＨＦＣ（Ｈｙｂｒｉｄ　ＦｉｂｅｒＣｏａｘ）を経由してヘッドエンドモデム３が接続される。

【００１９】ヘッドエンドモデム３はＣＡＴＶ局内に設けられ、サーバー４を経由してインターネットに接続される。サーバー４はケーブルモデム１のＩＣカード１０の登録を変更できる機能を有し、メールサーバー機能も有する。図３は図１又は図２におけるケーブルモデムの不正アクセス制限部１Ａの動作を説明するフローチャートである。

【００２０】本図に示すように、ステップＳ１において、ケーブルモデム１はＣＡＴＶ回線が通常運用状態にあることを確認する。ステップＳ２において、ケーブルモデム１は、ネットワーク側からケーブルモデム１配下のＰＣ２のアクセス要求を受信する。ステップＳ３において、ケーブルモデム１の不正アクセス制限部１Ａはケーブルモデム１にＩＣカード１０が挿入されているか否かを判断する。挿入されていない場合には、ステップＳ７に進む。

【００２１】この判断は、ＩＣカード１０の有無によるユーザ毎のサービス（セキュリティー機能の有無）の設定を可能にする。ステップＳ４において、ＩＣカード１０が挿入されている場合には、不正アクセス制限部１Ａは、アクセス要求元のＩＰアドレスがＩＣカード１０内

に登録されているアクセス許可のＩＰアドレスか否かを判断する。登録されていない場合にはステップＳ８に進む。

【００２２】ステップＳ５において、ＩＣカード１０内に許可すべきＩＰが登録されている場合には、不正アクセス制限部１Ａはケーブルモデム１の配下のＰＣ２へのアクセスを許可する。ステップＳ６において、不正アクセス制限部１Ａはデータをフォワードし、ステップＳ１に戻る。

【００２３】ステップＳ７において、ステップＳ３でＩＣカード１０の挿入がされていない場合には、不正アクセス制限部１Ａはアクセスを許可してステップＳ１に戻る。ステップＳ８において、ステップＳ４で、不正アクセス制限部１Ａは、アクセス要求元のＩＰアドレスがＩＣカード１０内に登録されているアクセス許可のＩＰアクセスと一致しない場合には、アクセスを拒否する。

【００２４】ステップＳ９において、不正アクセス制限部１Ａは受信したデータを廃棄し、ステップＳ１に戻る。この廃棄により、受信したデータにより悪影響を受ける可能性を回避するためである。図４は図１又は図２におけるケーブルモデムの不正アクセス制限部１Ａについて別の動作を説明するフローチャートである。

【００２５】本図に示すように、ステップＳ１１において、ケーブルモデム１はＣＡＴＶ回線が通常運用状態にあることを確認する。ステップＳ１２において、ケーブルモデム１は、ネットワーク側からケーブルモデム１の配下のＰＣ２へのアクセス要求を受信する。ステップＳ１３において、不正アクセス制限部１Ａは、アクセス要求元のＩＰアドレスがＩＣカード１０内に登録されているアクセス許可のＩＰアドレスと一致するか否かを判断する。一致する場合にはステップＳ１１に戻る。

【００２６】ステップＳ１４において、不正アクセス制限部１Ａは一致しない場合には、アクセスを拒否する。ステップＳ１５において、不正アクセス制限部１Ａは送信されてきたデータを廃棄する。ステップＳ１６において、不正アクセス制限部１Ａは、アクセス要求元のＩＰアドレスがＩＣカード１０の不正アクセス履歴テーブルに登録されているＩＰアドレスと一致するか否かを判断する。一致しない場合にはステップＳ２０に進む。

【００２７】ステップＳ１７において、不正アクセス制限部１Ａは、アクセス要求元のＩＰアドレスがＩＣカード１０の不正アクセス履歴テーブルに登録されているＩＰアドレスと一致する場合には、不正アクセス回数のインクリメントを行う。ステップＳ１８において、不正アクセス制限部１Ａは、不正アクセス回数が所定の閾値Ｎ回よりも大きいか否かを判断する。大きくない場合にはステップＳ１１に戻る。

【００２８】ステップＳ１９において、不正アクセス制限部１Ａは、不正アクセス回数が所定の閾値Ｎ回よりも大きい場合には管理者（サーバー４）に通知してステップＳ１１に戻る。ステップＳ２０において、不正アクセス制限部１Ａは、ステップＳ１６でアクセス要求元のＩＰアドレスが不正アクセス履歴テーブルに登録されていないＩＰアドレスと一致しない場合には、不正アクセス履歴テーブルにＩＰアドレスを登録して、ステップＳ１１に戻る。

【００２９】このように、繰り返し不正アクセスを行おうとするユーザを検出した場合には、サーバー（管理者）へ通知が行われる。この通知があると、サーバーは不正アクセスを行うユーザに警告等を行う。図５は図１又は図２におけるケーブルモデムの不正アクセス制限部１Ａについて他の動作を説明するフローチャートであり、図６は図５の機能を実現するシーケンスチャートである。

【００３０】図５に示すように、ステップＳ２１において、ケーブルモデム１はＣＡＴＶ回線が通常運用状態にあることを確認する。ステップＳ２２において、サーバー４は、ケーブルモデム１の配下のＰＣ２から、ケーブルモデム１、ＣＭＴＳ（Ｃａｂｌｅ　Ｍｏｄｅｍ　Ｔｅｒｍｉｎａｔｉｏｎ　Ｓｙｓｔｅｍ；ＣＡＴＶ局設備）を経由して、ＩＣカード１０の情報書き換え要求を受信する（図６参照）。

【００３１】ステップＳ２３において、サーバー４は、ケーブルモデム１にＩＣカード１０が挿入されているか否かの判断を行う（図６参照）。挿入されていない場合にはＩＣカード１０の書き換え要求を拒否しステップＳ２１に戻る。ステップＳ２４において、ケーブルモデム１にＩＣカード１０が挿入されている場合には、サーバー４は、ＩＣカード１０がユーザ自身のものかを判断する（図６参照）。一致しない場合には、ＩＣカード１０の情報書き換え要求を拒否し、ステップＳ２１に戻る。

【００３２】ステップＳ２５において、サーバー４は、ＩＣカード１０が登録されている所有ユーザ名ＩＤと一致する場合、ＩＣカード１０内のＩＰアドレス情報の追加、修正、削除等の書き換えを行って（図６参照）、ステップＳ２１に戻る。このように、サーバー４からの設定により、ＩＣカード１０内のアクセス許可ＩＰアドレスが自動設定される。

【００３３】このため、アクセス許可ＩＰアドレスの変更を容易に行うことができるようになった。

【００３４】

【発明の効果】以上説明したように、本発明によれば、複数台のヘッドエンドモデムがネットワーク内に存在する場合に、異なるヘッドエンドモデム配下のＰＣ間でアクセスの制限を行うようにしたので、不正アクセスを制限することが可能になった。

【図面の簡単な説明】

【図１】本発明に係るケーブルモデムへの不正アクセス制限システムの概略構成を示すブロック図である。

【図２】図１のケーブルモデム１に接続されるＣＡＴＶ

を説明する図である。

【図３】図１又は図２におけるケーブルモデム１の不正アクセス制限部１Ａの動作を説明するフローチャートである。

【図４】図１又は図２におけるケーブルモデム１の不正アクセス制限部１Ａについて別の動作を説明するフローチャートである。

【図５】図１又は図２におけるケーブルモデム１の不正アクセス制限部１Ａについて他の動作を説明するフローチャートである。

【図６】図５の機能を実現するシーケンスチャートである。

【図７】双方向ＣＡＴＶ回線を使ったネットワークを示す図である。

【符号の説明】

１…ケーブルモデム

１Ａ…不正アクセス制限部

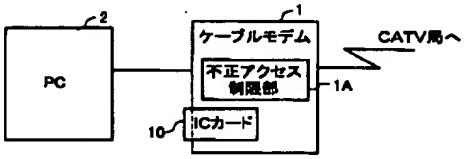
２…ＰＣ

３…ヘッドエンドモデム

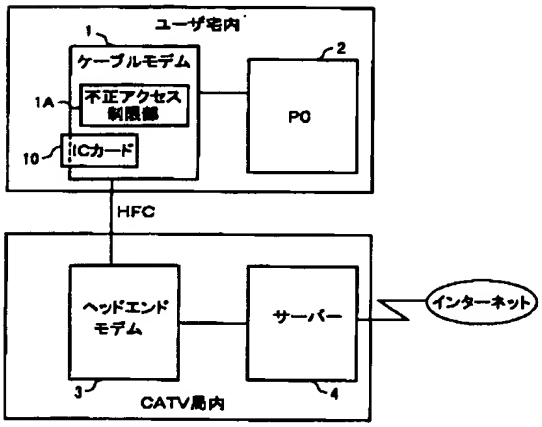
４…サーバー

１０…ＩＣカード

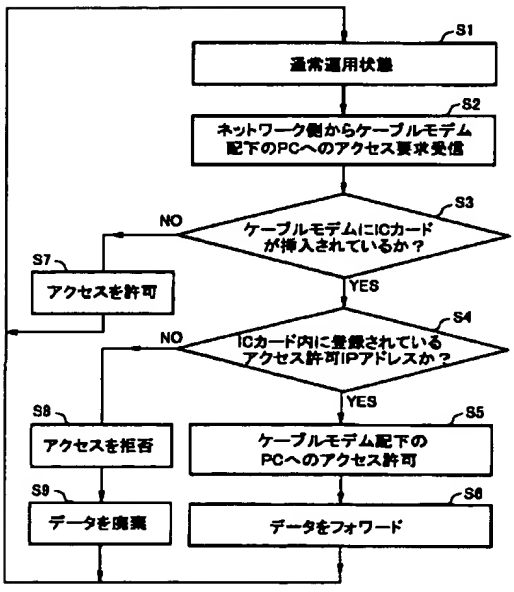
【図１】



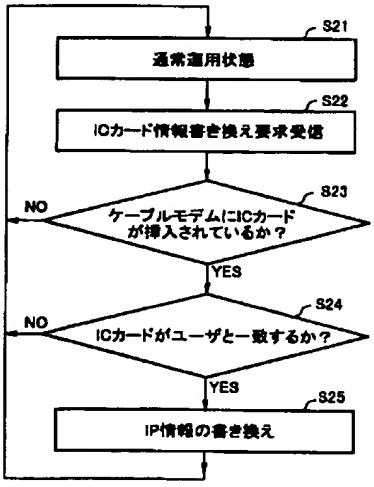
【図２】



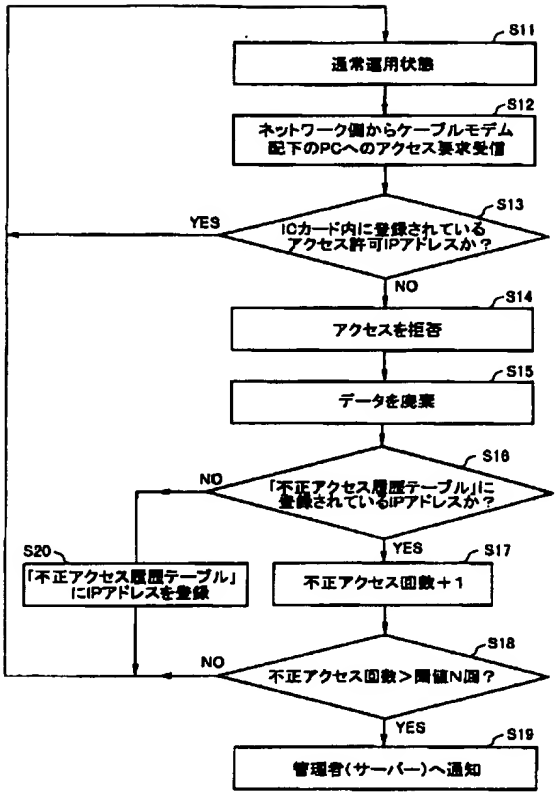
【図３】



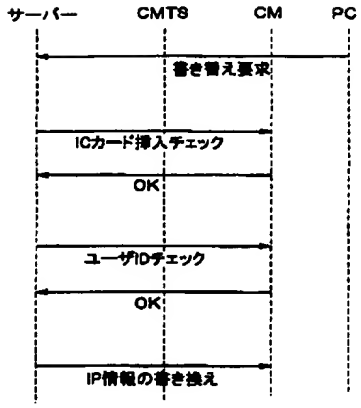
【図５】



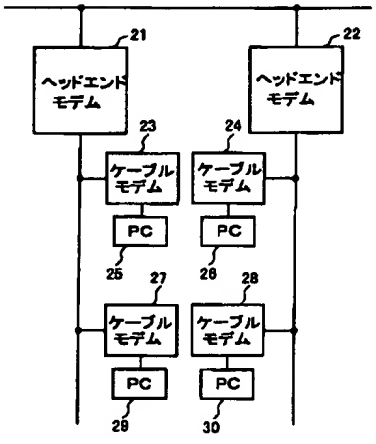
【図４】


S11
通常運用状態
S12
ネットワーク側からケーブルモデム配下のPCへのアクセス要求受信
S13
YES
ICカード内に登録されているアクセス許可IPアドレスか？
NO
S14
アクセスを拒否
S15
データを廃棄
S16
NO
「不正アクセス履歴テーブル」に登録されているIPアドレスか？
YES
S20
「不正アクセス履歴テーブル」にIPアドレスを登録
S17
不正アクセス回数＋１
S18
NO
不正アクセス回数＞閾値N回？
YES
S19
管理者（サーバー）へ通知

【図６】


サーバー
CMTS
CM
PC
書き換え要求
ICカード挿入チェック
OK
ユーザIDチェック
OK
IP情報の書き換え

【図７】


21
ヘッドエンドモデム
22
ヘッドエンドモデム
23
ケーブルモデム
24
ケーブルモデム
PC
PC
25
26
27
ケーブルモデム
28
ケーブルモデム
PC
PC
29
30